

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

FILED

JUL 13 2018

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

IN THE MATTER OF AN APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR A WARRANT TO OBTAIN)
RECORDS, LOCATION INFORMATION,)
INCLUDING PRECISION LOCATION)
INFORMATION, CELL SITE)
INFORMATION, AND OTHER)
SIGNALING INFORMATION)
ASSOCIATED WITH THE CELLULAR)
TELEPHONE HAVING THE NUMBERS)
(314) 203-7870.)

No. 4:18 MJ 3224 NCC

FILED UNDER SEAL

APPLICATION

COMES NOW the United States of America, by and through its attorneys, Jeffrey B. Jensen, United States Attorney for the Eastern District of Missouri, and Paul J. D'Agrosa, Assistant United States Attorney for said District, and hereby makes application to this Court for a warrant and order, pursuant to Title 18, United States Code, Sections 2703(c)(1)(A) and 3123, authorizing agents/officers of the UNITED STATES MARSHALS SERVICE (hereinafter referred to as "investigative agency(ies)"), and other authorized federal/state/local law enforcement agencies, to obtain records and location information, including precision location information, cell site location information, and other signaling information, associated with the following cellular telephone, which is further identified as follows:

TELEPHONE NO.: (314) 203-7870

ESN/IMSI NO.: UNKNOWN

SUBSCRIBER: UNKNOWN

ADDRESS: UNKNOWN

(hereinafter the "**subject cellular telephone**").

I. Introduction & Relief Requested

1. The undersigned applicant for the Government is an Assistant United States Attorney in the Office of the United States Attorney for the Eastern District of Missouri, and an "attorney for the Government," as defined in Fed. R. Crim. P. 1(b)(1)(B). Therefore, pursuant to Title 18, United States Code, Sections 2703(c) and 3122(a)(1), the undersigned may apply for an Order authorizing the disclosure of the telecommunication records and information requested herein.

2. The **subject cellular telephone** is serviced by T-MOBILE (hereinafter referred to as "the Service Provider"). The records and information requested herein are directed at location-related information and subscriber information associated with the **subject cellular telephone**, and may include information related to when the **subject cellular telephone** is located in a protected space, such as a residence. This application does not seek to compel or acquire the disclosure of the content of any communications.

3. The USMS has probable cause to believe that the **subject cellular telephone** is currently being used by NORRIS DOUGLAS, JR. who is charged with possession with intent to distribute fentanyl and, possession of a firearm in furtherance of a drug-trafficking crime in violation of Title 21, United States Code, Section 841(a)(1) and, Title 18, United States Code, Section 924(c)(1), in Case No. 4:18 CR 589 HEA DDN, and whose whereabouts are currently unknown.

4. The Government makes this application upon a showing of probable cause. Attached to this application and incorporated by reference as if fully set out herein is the affidavit of Deputy United States Marshal, Justin Barlow which alleges facts in order to show that there is

probable cause to believe that the location and arrest of NORRIS DOUGLAS, JR. can be obtained by locating and monitoring the location of the **subject cellular telephone**, without geographic limitation within the United States, including by obtaining precision location information (e.g., GPS information), cell site information, signaling information, and records concerning the **subject cellular telephone** for a period of forty-five (45) days measured from the date the Warrant is issued -- *i.e.*, from July 13, 2018, to August 26, 2018, 11:59 p.m. (CT).

5. The present application requests relief in three forms. First, the application requests relief in the form of precision location information, including GPS information, associated with the **subject cellular telephone**. Second, the application requests subscriber records and cell site information, which does not include precision location information, associated with the **subject cellular telephone**. Third, the application requests authorization for the installation and use of pen register and trap-and-trace devices.

II. Precision Location Information Request

1. The Government requests a warrant directing the Service Provider, any telecommunication service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications (herein incorporated by reference), and any other applicable service providers, to provide precision location information, including Global Position System (GPS) information, but not the contents of any communications, associated with the **subject cellular telephone**, for a period of forty-five (45) days from the date of any warrant issued hereon -- *i.e.*, from July 13, 2018, to August 26, 2018, 11:59 p.m. (CT).

2. The Service Provider is a service provider within the meaning of Title 18, United States Code, Section 2510(15), and as such, is subject to Title 18, United States Code, Section 2703(c)(1)(A) which states:

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record of other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure...by a court of competent jurisdiction....

3. The Court has jurisdiction to issue a warrant for the disclosure of precision location information, as requested herein, because it is "a court of competent jurisdiction," as defined in Title 18, United States Code, Sections 2711(3), and 2703(a), (b), and (c). Specifically, the Court has jurisdiction over the offense being investigated.

4. Title 18, United States Code, Section 2703(g) provides that an officer is not required to be present for the service or execution of a warrant issued under Section 2703. In particular, Section 2703(g) states:

Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber or customer of such service.

5. Title 18, United States Code, Section 2703(c)(3) permits the government to obtain the requested information and records without providing notice to any subscriber or customer. In particular, Section 2703(c)(3) states: "A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."

III. Cell Site Location Information Request

1. The Government requests a warrant directing the Service Provider, any telecommunication service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications, and any other applicable service providers, to provide certain telecommunication records and information, including cell site location information, but not the contents of any communication, for the time period of thirty (30) days prior to the warrant and for forty-five (45) days from the date of the requested warrant -- *i.e.*, from July 13, 2018, to August 26, 2018, 11:59 p.m. (CT). In particular, the Government requests the following telecommunication records and information:

(1) subscriber information and all telephone numbers, ESN, MIN, IMEI, MSID or IMSI numbers, including any and all customer service records, credit and billing

records, can-be-reached numbers (CBR), enhanced custom calling features, and primary long-distance carrier;

(2) subscriber information available for any originating telephone number;

(3) Automated Messaging Accounting (AMA) records (a carrier billing mechanism data base search which provides records of originating and terminating caller information for calls at the **subject cellular telephone**) for the above-specified time period;

(4) cellular telephone records and information pertaining to the following, for the above-specified time period:

(a) call detail information (provided in an electronic format specified by the agents/officers of the investigative agency(ies), and other authorized federal/state/local law enforcement agencies);

(b) cell site activation information, including information identifying the antenna tower receiving transmissions from the **subject cellular telephone** number, and any information on what portion of that tower is receiving a transmission from the **subject cellular telephone** number, at the beginning and end of a particular telephone call made to or received by the **subject cellular telephone** number;

(c) numbers dialed;

(d) call duration;

(e) incoming numbers if identified;

(f) signaling information pertaining to that number;

(g) a listing of all control channels and their corresponding cell sites;

(h) an engineering map showing all cell site tower locations, sectors and orientations; and

(i) subscriber information, including the names, addresses, credit and billing information, published and non-published for the telephone numbers being dialed from the **subject cellular telephone**.

(j) historical location estimates, such as Network Event Location System (NELOS), round-trip time (RTT), GPS, and per-call measurement data (PCMD) and

(k) Internet Protocol (IP addresses) utilized by and signaled to and from the **subject cellular telephone**.

2. The Service Provider is a service provider within the meaning of Title 18, United States Code, Section 2510(15), and as such, is subject to Title 18, United States Code, Section 2703(c)(1)(A) which states:

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record of other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure...by a court of competent jurisdiction....

3. The Court has jurisdiction to issue a warrant for the disclosure of requested telecommunications records, including cell site records because it is "a court of competent jurisdiction," as defined in Title 18, United States Code, Sections 2711(3), and 2703(a), (b), and (c). Specifically, the Court has jurisdiction over the offense being investigated.

4. Title 18, United States Code, Section 2703(g) provides that an officer is not required to be present for the service or execution of a warrant issued under Section 2703. In particular, Section 2703(g) states:

Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber or customer of such service.

5. Title 18, United States Code, Section 2703(c)(3) permits the government to obtain the requested information and records without providing notice to any subscriber or customer. In particular, Section 2703(c)(3) states: "A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."

IV. Pen Register, Trap-and-Trace Request

1. The Government's application seeks an Order, pursuant to Title 18, United States Code, Section 3122, authorizing the installation and use of pen register and trap-and-trace devices, including enhanced caller identification, as defined in Title 18, United States Code, Section 3127, without geographic limitation within the United States, and including an Order authorizing the installation and use of a pen register to record or decode dialing, routing, addressing, or signaling information transmitted by the **subject cellular telephone** number further identified herein, and a trap-and-trace device, including enhanced caller identification, which captures the incoming

electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication to and from the **subject cellular telephone** number, direct connect, Voice-over-LTE (VoLTE), non-content data transmissions, or digital dispatch dialings (if applicable), the dates and times of such dialings, and the length of time of the connections, for the time period from July 13, 2018, to August 26, 2018, 11:59 p.m. (CT).

2. In making this application, the Government does not seek the contents of any communication, such that other legal process would be required.

3. As previously outlined, the Government certifies that the information likely to be obtained through the aforesaid pen register and trap-and-trace devices, including enhanced caller identification, is relevant to an ongoing criminal investigation.

4. The Government further requests that the Order direct the telecommunications service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications, here incorporated by reference, and any other applicable service providers, to initiate caller identification on the subject cellular telephone number listed above, without the knowledge of or notification to the subscriber, for the purpose of registering incoming telephone numbers.

5. The Government further requests that the Order direct the furnishing of information, facilities, and technical assistance, as necessary, to unobtrusively accomplish the installation and use of the pen register and trap-and-trace devices, including enhanced caller identification, by the telecommunications service providers reflected in Attachment 1, to include

providers of any type of wire and/or electronic communications and any other applicable service providers, and with a minimum of disruption of normal telephone service.

6. The Government further requests that the Order direct that the results of the pen register and trap-and-trace devices, including enhanced caller identification, be provided to the agents/officers of the investigative agency(ies) at reasonable intervals for the duration of the Order.

V. Changed Numbers, Compensation and Sealing

1. The Government requests that should the subject cellular telephone and/or ESN, MIN, IMEI, MSID or IMSI number listed above be changed by the subscriber during the effective period of any Order granted as a result of this application, that the Court order the request for pen register and trap-and-trace devices remain in effect for any new telephone to which the subject cellular telephone listed above is changed, throughout the effective period of such Order.

2. The Government further requests that the Order direct that the lead investigative agency provide the telecommunications service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications, and any other applicable service providers, just compensation for reasonable expenses incurred in providing such information, facilities and technical assistance.

VI. Sealing, Notification and Miscellaneous Considerations

1. Pursuant to Title 18, United States Code, Section 2703, the Government requests that the Court direct that the telecommunications service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications, and any other applicable service providers, shall provide the agents/officers of the investigative agency(ies), and other authorized federal/state/local law enforcement agencies, with the following:

- (1) subscriber information;
- (2) length of service (including start date);
- (3) the types of service utilized;
- (4) instrument number or other subscriber number or identity, including any temporarily assigned network address;
- (5) all available names, addresses, and identifying information, and other subscriber and service feature information;
- (6) toll records including incoming and outgoing telephone numbers;
- (7) credit information, billing information, and air-time summaries for available service periods, for the IP (internet protocol) addresses being utilized by and signaled to and from the aforementioned subject cellular telephone,

for the telephone numbers being dialed to and from the aforementioned **subject cellular telephone** at reasonable intervals for the past thirty (30) days from the date of this Warrant and at reasonable intervals for up to forty-five (45) days from the date of this Warrant -- *i.e.*, from July 13, 2018, to August 26, 2018, 11:59 p.m. (CT).

2. Pursuant to Title 18, United States Code, Section 2703(c)(3), the Government entity or agency receiving these records or information as a result of this application and accompanying warrant and order will not provide notice to the subscriber or customer of the **subject cellular telephone**.

3. This Court has authority under Title 18, U.S.C., Section 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems

appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.*

4. In this case, such an order is appropriate because the Government seeks the warrant in part under the authority granted to this court pursuant to Title 18, U.S.C., Section 2703. The requested warrant is related to an ongoing criminal investigation that is not public and this portion of the investigation is not known to the subjects of the investigation. Premature notification may alert the subject(s) to the existence of the investigation. If the subjects were notified about the existence of the requested warrant, the subjects could destroy evidence. Accordingly, there is reason to believe that notification of the existence of the warrant will seriously jeopardize the investigation, including giving the subjects an opportunity to: flee, destroy and/or tamper with evidence; change patterns of behavior; or notify confederates. *See* Title 18, U.S.C., Section 2705(b)(2), (3), and (5). Based on the nature and circumstances of the investigation, there is also reason to believe that notification of the existence of the warrant will result in endangering the life or physical safety of an individual, or the intimidation of potential witnesses. *See* Title 18, U.S.C., Section 2705(b)(1) and (4).

5. Based on the foregoing, pursuant to Title 18, United States Code, Sections 3123(d)(1) and (2) and 2705(b), the Government requests that the Court direct the Service Provider and the telecommunications service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications, and any other applicable service providers, not to disclose the existence of this application and/or any warrant or order issued upon this application, or the existence of the investigation, for a period of one year from the date of this

Order, to a subscriber or lessee or to any other person, except that the provider may disclose the warrant and any Order to an attorney for the provider for the purpose of receiving legal advice.

6. The information requested herein does not require a physical intrusion or physical trespass into any protected space. Accordingly, it is respectfully requested that the warrant authorize the investigative agency(ies), and other authorized federal/state/local law enforcement agencies, to obtain the location information described herein at any time, day or night.

7. The Government further requests that the Order direct that the investigative agency(ies) provide the telecommunication providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications, and any other applicable service providers, just compensation for reasonable expenses incurred in providing such information, facilities and technical assistance.

8. In light of the ongoing nature of the investigation as reflected in the attached affidavit, and because disclosure at this time would seriously jeopardize the investigation, including by giving the subject(s) an opportunity to destroy and/or tamper with evidence and flee, applicant requests that the application, affidavit and warrant be sealed.

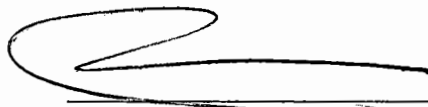
WHEREFORE, on the basis of the allegations contained in this application, and on the basis of the affidavit of Deputy United States Marshal, Justin Barlow, which is attached hereto and made a part hereof, applicant requests this Court to issue a Warrant authorizing agents/officers of the UNITED STATES MARSHALS SERVICE (the investigative agency(ies)), and other authorized federal/state/local law enforcement agencies, to obtain location information, including precision location information, cell site location information, and other signaling information associated with the **subject cellular telephone.**

I declare under penalty of perjury that the foregoing is true and correct to the best of my current knowledge, information, and belief.

Dated this 13th day of July, 2018.

Respectfully submitted,

JEFFREY B. JENSEN
United States Attorney

A handwritten signature in black ink, appearing to read 'PAUL J. D'AGROSA', written over a horizontal line.

PAUL J. D'AGROSA, #36966MO
Assistant United States Attorney

LIST OF TELECOMMUNICATION SERVICE PROVIDERS**T-MOBILE**

and

01 Communications	Egyptian Telephone	Mid-Atlantic	Socket Telecom
Access Line Communication	Electric Lightwave, Inc.	Midvale Telephone Exchange	Spectrum
ACN, Inc.	Empire Paging	Mobile Communications	Sprint
ACS	Ernest Communications	Mound Bayou Telephone Co.	SRT Wireless
Aero Communications, Inc. (IL)	EZ Talk Communications	Mpower Communications	Star Telephone Company
Afford A Phone	FDN Communications	Navigator	Start Wireless
Airvoice Wireless	Fibernet Comm	Telecommunications	Sugar Land Telephone
Alaska Communications	Florida Cell Service	NE Nebraska Telephone	Sure West Telephone Company
Alhambra-Grantfx Telephone	Florida Digital Network	Netlink Comm	Talk America
Altice USA	Focal Communications	Network Services	Tele Touch Comm
AmeriTel	Frontier Communications	Neustar	Telecorp Comm
AOL Corp.	FuzeBox, Inc.	Neutral Tandem	Telepak
Arch Communication	Gabriel Comm	Nex-Tech Wireless	Telispire PCS
AT&T	Galaxy Paging	Nexus Communications	Telnet Worldwide
AT&T Mobility	Global Communications	NII Comm	Tex-Link Comm
Bell Aliant	Global Eyes Communications	North Central Telephone	Time Warner Cable
Big River Telephone	Global Naps	North State Comm	T-Mobile
Birch Telecom	Grafton Telephone Company	Northcoast Communications	Total Call International
Blackberry Corporation	Grand River	Novacom	Tracfone Wireless
Brivia Communications	Grande Comm	Ntera	Trinity International
Broadview Networks	Great Plains Telephone	NTS Communications	U-Mobile
Broadvox Ltd.	Harrisonville Telephone Co.	Oklahoma City SMSA	United Telephone of MO
Budget Prepay	Heartland Communications	ONE Communications	United Wireless
Bulls Eye Telecom	Hickory Telephone	ONSTAR	US Cellular
Call Wave	Huxley Communications	Optel Texas Telecom	US Communications
Cbeyond Inc.	iBasis	Orion Electronics	US LEC
CCPR Services	IDT Corporation	PacBell	US Link
Celloo Partnership, d/b/a Verizon Wireless	Illinois Valley Cellular	PacWest Telecom	US West Communications
Cellular One	Insight Phone	PAETEC Communications	USA Mobility
Cellular South	Integra	Page Plus Communications	VarTec Telecommunications
Centennial Communications	Iowa Wireless	Page Mart, Inc.	Verisign
CenturyLink	IQ Telecom	Page Net Paging	Verizon Telephone Company
Charter Communications	J2 Global Communications	Panhandle Telephone	Verizon Wireless
Chickasaw Telephone	Leap Wireless International	Peerless Network	Viaero Wireless
Choctaw Telephone Company	Level 3 Communications	Pineland Telephone	Virgin Mobile
Cimco Comm	Locus Communications	PhoneTech	Vonage Holdings
Cincinnati Bell	Logix Communications	PhoneTel	Wabash Telephone
Cinergy Communications	Longlines Wireless	Preferred Telephone	Wave2Wave Communications
Clear World Communication	Los Angeles Cellular	Priority Communications	Weblink Wireless
Com-Cast Cable Comm.	Lunar Wireless	Puretalk	Western Wireless
Commercial Communications	Madison River	RCN Telecom	Westlink Communications
Consolidated Communications	Communications	RNK Telecom	WhatsApp
Cox Communications	Madison/Macoupin Telephone Company	QWEST Communications	Windstream Communications
Cricket Wireless	Mankato Citizens Telephone	Sage Telecom	Wirefly
Custer Telephone Cooperative	Map Mobile Comm	Seren Innovations	XFINITY
DBS Communications	Marathon Comm	Shentel	XO Communications
Delta Communications	Mark Twain Rural	Sigecom LLC	Xspedius
Detroit Cellular	Max-Tel Communications	Sky Tel Paging	Yakdin Valley Telephone
Dobson Cellular	Metro PCS	Smart Beep Paging	YMAX Communications
	Metro Teleconnect	Smart City Telecom	Ztel Communications

**ATTACHMENT 1, TO INCLUDE PROVIDERS OF ANY TYPE OF WIRE AND/OR
ELECTRONIC COMMUNICATIONS**

Last Update: 06/21/2018

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

FILED

JUL 13 2018

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

IN THE MATTER OF AN APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR A WARRANT TO OBTAIN)
RECORDS, LOCATION INFORMATION,)
INCLUDING PRECISION LOCATION)
INFORMATION, CELL SITE)
INFORMATION, AND OTHER)
SIGNALING INFORMATION)
ASSOCIATED WITH THE CELLULAR)
TELEPHONE HAVING THE NUMBERS)
(314) 203-7870.)

No. 4:18 MJ 3224 NCC

FILED UNDER SEAL

AFFIDAVIT

Justin Barlow, being duly sworn, deposes and says that he is a Deputy United States Marshal with the United States Marshals Service, duly appointed according to law and acting as such.

Introduction

Your Affiant is a Deputy United States Marshal (DUSM) and has been so employed since November 2010. Prior to joining the United States Marshals Service, your affiant worked as a police officer for the Columbia, Illinois Police Department for ten years. As a police officer with Columbia, this Affiant worked as a patrol officer for four years, and an investigator for six years. This Affiant served as an Investigator with the Major Case Squad of the Greater St. Louis Area assisting in the investigation of approximately twenty homicides. Your Affiant served as a Special Federal Officer with the Cyber Crime Task Force with the Federal Bureau of Investigation in Fairview Heights, Illinois for five years with duties that included investigating computer crimes such as computer fraud, identity theft, computer intrusion, and child pornography. As a member

of the task force this Affiant received top secret security clearance through the Federal Bureau of Investigation. Your Affiant has a Bachelor's degree from Saint Louis University. This Affiant graduated the Southwestern Illinois College Police Academy in 2000 and is also a graduate of the United States Marshals Service basic academy and the Criminal Investigator Training Program from the Federal Law Enforcement Training Center, Glynco, GA. My current duty assignment is in the Eastern District of Missouri. My primary duty and assignment obligates me to investigative, locate, and apprehend state and federal fugitives.

The facts alleged in this affidavit come from my own investigation, my training and experience, and information obtained from other investigators and witnesses. As this affidavit is submitted for the limited purpose of establishing probable cause to locate and monitor the location of a cellular telephone as part of a criminal investigation, it does not set forth all of the my knowledge regarding this matter.

Upon information and belief, and as explained in greater detail below, the cellular telephone bearing number (314) 203-7870 (hereinafter the "**subject cellular telephone**"), which is being serviced by T-MOBILE (hereinafter referred to as "the Service Provider"), has been used, and is presently being used, in connection with the commission of offenses involving ongoing violations of Title 21, United States Code, Section 841(a)(1) and, Title 18, United States Code, Section 924(c)(1) (hereinafter referred to as "the subject offenses"), by NORRIS DOUGLAS, JR. who is charged with possession with intent to distribute fentanyl and, possession of a firearm in furtherance of a drug-trafficking crime in violation of Title 21, United States Code, Section 841(a)(1) and, Title 18, United States Code, Section 924(c)(1), in Case No. 4:18 CR 589 HEA DDN, and whose whereabouts are currently unknown.

The present affidavit is being submitted in connection with an application of the Government for a warrant and order authorizing agents/officers of the investigative agency(ies), and other authorized federal/state/local law enforcement agencies, to obtain location information, including precision location information, cell site location information, and other signaling information, including pen register information, in an effort to locate and monitor the location of the **subject cellular telephone**.

Your affiant further states that there is probable cause to believe that the location information associated with the **subject cellular telephone** will lead to the location and arrest of NORRIS DOUGLAS, JR..

Investigation and Probable Cause

On June 15, 2017, in the Eastern District of Missouri, an arrest warrant was issued for **DOUGLAS**, charging the aforementioned criminal violations, based on a criminal complaint. **DOUGLAS** was arrested and brought before the court. On June 27, 2018, **DOUGLAS** waived a detention hearing and was committed to custody by United States Magistrate Judge John BODENHAUSEN. On July 3, 2018, **DOUGLAS** was erroneously released from custody from the St. Louis County Justice Center. The Court, as well as the United States Marshals Service, learned of the erroneous release on or about July 9, 2018. The United States Marshals Service subsequently initiated a fugitive investigation for **DOUGLAS**.

On July 11, 2018, in the Eastern District of Missouri, **DOUGLAS** was indicted by an empaneled grand jury for the aforementioned narcotics violations.

On July 11, 2018, United States Marshals Service investigators conducted a number of consensual interviews of relatives and associates of **DOUGLAS**, in an effort to locate and arrest

DOUGLAS. In one such interview, investigators interviewed **DOUGLAS**' estranged wife, Ashley **DOUGLAS**. Ashley **DOUGLAS** indicated she was not longer in a romantic relationship with **DOUGLAS**, and consented to a search of her residence. **DOUGLAS** was not located. Investigators also identified a girlfriend of **DOUGLAS**, identified as Wil'lisha **WELFORD**. Investigators endeavored to locate **WELFORD**; first at her address of record, and later at her place of employment. The efforts to locate **WELFORD** at her residence were unsuccessful, but investigators spoke with a neighbor who confirmed **WELFORD** and **DOUGLAS** lived at the residence. Investigators were later able to make contact with **WELFORD** at her place of employment. Subsequent consensual interview of **WELFORD** failed to generate any substantive leads with respect to **DOUGLAS**' whereabouts. Investigators, based on previous investigative measures, were able to determine **WELFORD** gave investigators inconsistent answers to their questioning, and the investigators suspected she was being untruthful.

On July 12, 2018, USMS investigators conducted surveillance at both **WELFORD**'s residence, as well as that of **WELFORD**'s sister, Diamond **BAUCOM**. **WELFORD**'s vehicle was observed parked at **BAUCOM**'s residence. Investigators made contact with **BAUCOM**, who also indicated she was unaware of **DOUGLAS**' whereabouts. **BAUCOM** also consented to a search of her residence, whereby neither **DOUGLAS** nor **WELFORD** were found. **BAUCOM** was later detained; based both on a number of outstanding local arrest warrants, as well as statements indicating **BAUCOM** and **WELFORD** were endeavoring to circumvent surveillance by the USMS by moving **WELFORD**'s vehicle to misdirect USMS surveillance. Investigators again went to **WELFORD**'s residence, where the aforementioned neighbor indicated she had seen **WELFORD**, accompanied by an unidentified man and woman, enter the home the previous

evening after arriving in WELFORD's vehicle. Believing WELFORD and **DOUGLAS** to be inside the residence, investigators forced entry to the residence. No one was found to be home. Investigators again located WELFORD at her place of employment and she was detained. After being advised of their constitutional rights, both WELFORD and BAUCOM were unable to provide the USMS investigators with any substantive information concerning **DOUGLAS'** whereabouts. WELFORD did indicate **DOUGLAS** had made statements to her indicating he was aware he was wanted by the USMS, and was attempting to avoid capture. WELFORD indicated it was her belief **DOUGLAS** was distrustful and WELFORD believed **DOUGLAS** was hiding out.

Finally, investigators conducted an arrest attempt at a residence associated with a friend of **DOUGLAS**. A consensual search of that residence was also unsuccessful in locating **DOUGLAS**.

USMS investigators also spoke with St. Louis County Police Department detectives whose investigation had given rise to the aforementioned criminal complaint and subsequent indictment. The detectives told USMS investigators they had extensive dealings and background knowledge, in furtherance of the narcotics investigation of **DOUGLAS**, of **DOUGLAS'** friends, family, and associates. The detectives also indicated they had a Confidential Source ("CS") who had provided consistently reliable information concerning **DOUGLAS** and others on numerous occasions. USMS investigators requested the detectives contact the CS in an effort to ascertain any relevant information concerning **DOUGLAS'** whereabouts.

The detectives later contacted USMS investigators and indicated the CS had spoken with associates, and eventually came into telephonic contact with **DOUGLAS** via the **Subject Cellular Telephone** on July 12, 2018. The CS indicated they definitively knew the voice to be that of

DOUGLAS, and the context of the conversation and information provided to the CS indicated the **Subject Cellular Telephone** was in **DOUGLAS**' possession as his primary telephonic means of communication, and that the **Subject Cellular Telephone** had been obtained by **DOUGLAS** at some point after his erroneous release.

The monitoring of cellular data, as well as the activation of precision location information, will permit investigators to ascertain who **DOUGLAS** is communicating with, as well as determine **DOUGLAS**' whereabouts. This information is believed to be the most efficacious in locating and arresting **DOUGLAS**.

The investigation has clearly demonstrated that the **subject cellular telephone** is being used by NORRIS DOUGLAS, JR. who is charged possession with intent to distribute fentanyl and, possession of a firearm in furtherance of a drug-trafficking crime in violation of Title 21, United States Code, Section 841(a)(1) and, Title 18, United States Code, Section 924(c)(1), in Case No. 4:18 CR 589 HEA DDN, and whose whereabouts are currently unknown. It is critical that the investigative team be able to locate and monitor the movements of the **subject cellular telephone** thereby assisting in the location and arrest of NORRIS DOUGLAS, JR.. Your affiant believes that the requested authorization would be a valuable asset in achieving the overall goals of the investigation.

Investigative Considerations and Techniques

Based on my knowledge, training, and experience, as well as information provided by investigators with specialized experience relating to cellular telephone technology, I am aware of the following facts and considerations:

A. Wireless phone providers typically generate and retain certain transactional information about the use of each telephone call, voicemail, and text message on their system. Such information can include log files and messaging logs showing all activity on a particular account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or other addressing information associated with particular telephone calls, voicemail messages, and text or multimedia messages.

B. Wireless phone providers also typically generate and retain information about the location in which a particular communication was transmitted or received. For example, when a cellular device is used to make or receive a call, text message or other communication, the wireless phone provider will typically generate and maintain a record of which cell tower(s) was/were used to process that contact. Wireless providers maintain information, including the corresponding cell towers (i.e., tower covering specific geographic areas), sectors (i.e., faces of the towers), and other signaling data as part of their regularly conducted business activities. Typically, wireless providers maintain records of the cell tower information associated with the beginning and end of a call.

C. Because cellular devices generally attempt to communicate with the closest cell tower available, cell site location information from a wireless phone provider allows investigators

to identify an approximate geographic location from which a communication with a particular cellular device originated or was received.

D. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers.

E. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscriber's full name and address, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscriber's Social Security Number and date of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscriber. In addition, wireless providers typically generate and

retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

F. Providers of cellular telephone service also typically have technical capabilities that allow them to collect and generate more precise location information than that provided by cell site location records. This information is sometimes referred to as E-911 phase II data, GPS data or latitude-longitude data. In the Eastern District of Missouri, such information is often referred to as "precision location information" or "PLI" data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by attempting to triangulate the device's signal using data from several of the provider's cell towers. Depending on the capabilities of the particular phone and provider, E-911 data can sometimes provide precise information related to the location of a cellular device.

In order to locate the **subject cellular telephone** and monitor the movements of the phone, the investigative agency(ies), and other authorized federal/state/local law enforcement agencies, may need to employ one or more techniques described in this affidavit and in the application of the government. The investigative agency(ies), and other authorized federal/state/local law enforcement agencies, may seek a warrant to compel the Service Provider, any telecommunication service providers reflected in Attachment 1, to include providers of any type of wire and/or electronic communications (herein incorporated by reference), and any other applicable service providers, to provide precision location information, including Global Position System

information (if available), transactional records, including cell site location information, and pen register and trap-and-trace data.

None of the investigative techniques that may be employed as a result of the present application and affidavit require a physical intrusion into a private space or a physical trespass. Electronic surveillance techniques such as pen register and cell site location monitoring typically have not been limited to daytime use only. Furthermore, the criminal conduct being investigated is not limited to the daytime. Therefore, the fact that the present application requests a warrant based on probable cause should not limit the use of the requested investigative techniques to daytime use only. Accordingly, the investigative agency(ies), and other authorized federal/state/local law enforcement agencies, request the ability to employ these investigative techniques at any time, day or night.

The monitoring of the location of the **subject cellular telephone** by one of the methods described herein will begin within ten (10) days of the date of issuance of the requested Warrant and Order.

Conclusion


Based on the above information, there is probable cause to believe that the **subject cellular telephone** is being used by NORRIS DOUGLAS, JR., who is charged possession with intent to distribute fentanyl and, possession of a firearm in furtherance of a drug-trafficking crime in violation of Title 21, United States Code, Section 841(a)(1) and, Title 18, United States Code, Section 924(c)(1), in Case No. 4:18 CR 589 HEA DDN, and whose whereabouts are currently unknown. There is likewise probable cause to conclude that locating and monitoring the

movements of the **subject cellular telephone** will lead to the location and arrest of NORRIS

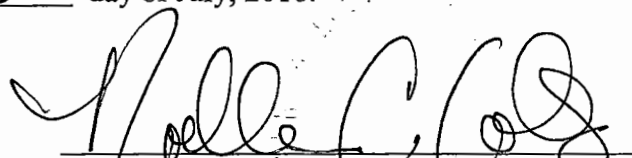
DOUGLAS, JR.

DATE

07/13/18


JUSTIN BARLOW
DEPUTY UNITED STATES MARSHAL
UNITED STATES MARSHALS SERVICE

Sworn to and subscribed before me this 13th day of July, 2018.


HONORABLE NOELLE C. COLLINS
UNITED STATES MAGISTRATE JUDGE
Eastern District of Missouri

LIST OF TELECOMMUNICATION SERVICE PROVIDERS**T-MOBILE**

and

01 Communications	Egyptian Telephone	Mid-Atlantic	Socket Telecom
Access Line Communication	Electric Lightwave, Inc.	Midvale Telephone Exchange	Spectrum
ACN, Inc.	Empire Paging	Mobile Communications	Sprint
ACS	Ernest Communications	Mound Bayou Telephone Co.	SRT Wireless
Aero Communications, Inc. (IL)	EZ Talk Communications	Mpower Communications	Star Telephone Company
Afford A Phone	FDN Communications	Navigator	Start Wireless
Airvoice Wireless	Fibernet Comm	Telecommunications	Sugar Land Telephone
Alaska Communications	Florida Cell Service	NE Nebraska Telephone	Sure West Telephone Company
Alhambra-Grantfx Telephone	Florida Digital Network	Netlink Comm	Talk America
Altice USA	Focal Communications	Network Services	Tele Touch Comm
AmeriTel	Frontier Communications	Neustar	Telecorp Comm
AOL Corp.	FuzeBox, Inc.	Neutral Tandem	Telepak
Arch Communication	Gabriel Comm	Nex-Tech Wireless	Telispire PCS
AT&T	Galaxy Paging	Nexus Communications	Telnet Worldwide
AT&T Mobility	Global Communications	NII Comm	Tex-Link Comm
Bell Aliant	Global Eyes Communications	North Central Telephone	Time Warner Cable
Big River Telephone	Global Naps	North State Comm	T-Mobile
Birch Telecom	Grafton Telephone Company	Northcoast Communications	Total Call International
Blackberry Corporation	Grand River	Novacom	Tracfone Wireless
Brivia Communications	Grande Comm	Ntera	Trinity International
Broadview Networks	Great Plains Telephone	NTS Communications	U-Mobile
Broadvox Ltd.	Harrisonville Telephone Co.	Oklahoma City SMSA	United Telephone of MO
Budget Prepay	Heartland Communications	ONE Communications	United Wireless
Bulls Eye Telecom	Hickory Telephone	ONSTAR	US Cellular
Call Wave	Huxley Communications	Optel Texas Telecom	US Communications
Cbeyond Inc.	iBasis	Orion Electronics	US LEC
CCPR Services	IDT Corporation	PacBell	US Link
Cellco Partnership, d/b/a Verizon Wireless	Illinois Valley Cellular	PacWest Telecom	US West Communications
Cellular One	Insight Phone	PAETEC Communications	USA Mobility
Cellular South	Integra	Page Plus Communications	VarTec Telecommunications
Centennial Communications	Iowa Wireless	Page Mart, Inc.	Verisign
CenturyLink	IQ Telecom	Page Net Paging	Verizon Telephone Company
Charter Communications	J2 Global Communications	Panhandle Telephone	Verizon Wireless
Chickasaw Telephone	Leap Wireless International	Peerless Network	Viaero Wireless
Choctaw Telephone Company	Level 3 Communications	Pineland Telephone	Virgin Mobile
Cimco Comm	Locus Communications	PhoneTech	Vonage Holdings
Cincinnati Bell	Logix Communications	PhoneTel	Wabash Telephone
Cinergy Communications	Longlines Wireless	Preferred Telephone	Wave2Wave Communications
Clear World Communication	Los Angeles Cellular	Priority Communications	Weblink Wireless
Com-Cast Cable Comm.	Lunar Wireless	Puretalk	Western Wireless
Commercial Communications	Madison River	RCN Telecom	Westlink Communications
Consolidated Communications	Communications	RNK Telecom	WhatsApp
Cox Communications	Madison/Macoupin Telephone Company	QWEST Communications	Windstream Communications
Cricket Wireless	Mankato Citizens Telephone	Sage Telecom	Wirefly
Custer Telephone Cooperative	Map Mobile Comm	Seren Innovations	XFINITY
DBS Communications	Marathon Comm	Shentel	XO Communications
Delta Communications	Mark Twain Rural	Sigecom LLC	Xspedius
Detroit Cellular	Max-Tel Communications	Sky Tel Paging	Yakdin Valley Telephone
Dobson Cellular	Metro PCS	Smart Beep Paging	YMAX Communications
	Metro Teleconnect	Smart City Telecom	Ztel Communications

**ATTACHMENT 1, TO INCLUDE PROVIDERS OF ANY TYPE OF WIRE AND/OR
ELECTRONIC COMMUNICATIONS**

Last Update: 06/21/2018